Patent Application Publication

DE 197 23 332 A 1

(54) Process for protection of a microcomputer and a protected microcomputer

(57) A process for protection of a microcomputer against manipulation of its program and a microcomputer which is protected in this way are proposed. The microcomputer (1) has a computer kernel (2), a read-only memory (3), and a rewritable memory (5). In the read-only memory (3) a checking program is stored which by means of a key generates a code word from the memory contents of the rewritable memory (5). The code word is then compared to a comparison code word which is likewise stored in the rewritable memory (5). Depending on this comparison the microcomputer is blocked or released.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 197 23 332 A 1**

(51) Int. Cl.[6]: G 06 F 12/14

(21) Aktenzeichen: 197 23 332.5
(22) Anmeldetag: 4. 6. 97
(43) Offenlegungstag: 3. 9. 98

DE 197 23 332 A 1

Mit Einverständnis des Anmelders offengelegte Anmeldung gemäß § 31 Abs. 2 Ziffer 1 PatG

(71) Anmelder:
Robert Bosch GmbH, 70469 Stuttgart, DE

(72) Erfinder:
Fischer, Werner, 71296 Heimsheim, DE;
Schoenfelder, Dietbert, 70839 Gerlingen, DE;
Barbehoen, Kai-Lars, 71634 Ludwigsburg, DE

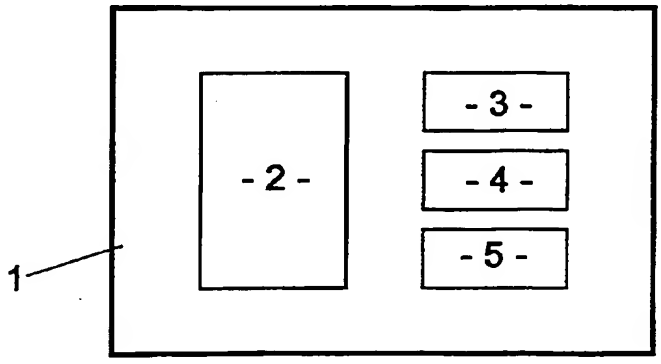
(56) Entgegenhaltungen:
DE 69 0 21 93 5T2

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zum Schutz eines Mikrorechners und geschützter Mikrorechner

(57) Es wird ein Verfahren zum Schutz eines Mikrorechners gegen Manipulation seines Programms bzw. ein derart geschützter Mikrorechner vorgeschlagen. Der Mikrorechner (1) weist einen Rechnerkern (2) einen nur Lesespeicher (3) und einen wiederbeschreibbaren Speicher (5) auf. Im nur Lesespeicher (3) ist ein Überprüfungsprogramm gespeichert, das mittels eines Schlüssels aus dem Speicherinhalt des wiederbeschreibbaren Speichers (5) ein Codewort bildet. Das Codewort wird dann mit einem Vergleichscodewort verglichen, das ebenfalls im wiederbeschreibbaren Speicher (5) abgelegt ist. In Abhängigkeit von diesem Vergleich wird der Mikrorechner gesperrt oder freigegeben.



DE 197 23 332 A 1

Beschreibung

Stand der Technik

Die Erfindung geht aus von einem Verfahren zum Schutz eines Mikrorechners bzw. einem geschützten Mikrorechner nach der Gattung der unabhängigen Patentansprüche. Es sind bereits Verfahren zum Schutz von Mikrorechner und geschützte Mikrorechner bekannt, die einen nur Lesespeicher und einen wiederbeschreibbaren Speicher aufweisen. Dabei wird im wiederbeschreibbaren Speicher ein Programm gespeichert. Um dieses Programm vor einer unerlaubten Manipulation zu schützen, werden die Befehle des Mikrorechners, die sich auf eine Veränderung des Speicherinhaltes richten, besonders geschützt. Derartige Befehle werden nur dann von dem Mikrorechner ausgeführt, wenn zuvor eine Zugriffsberechtigung durch ein Paßwort verifiziert wurde. Weiterhin ist es bekannt den Speicherinhalt eines wiederbeschreibbaren Speichers dadurch zu schützen, daß an mehreren Stellen im Speicher Checksummen über einen gewissen Speicherbereich abgelegt sind. Bei der Ausführung des Programms werden dann diese Checksummen mit dem Inhalt der Speicherbereiche verglichen, so daß eine teilweise Veränderung des Speicherinhalts nur dann erfolgreich ist, wenn gleichzeitig auch die Checksummen verändert werden.

Wenn jedoch die Speicherplätze auf denen die Checksummen abgelegt werden bekannt sind, kann eine Manipulation des Speicherinhalts nicht verhindert werden.

Vorteile der Erfindung

Das erfindungsgemäße Verfahren zum Schutz eines Mikrorechners bzw. der erfindungsgemäße geschützte Mikrorechner haben demgegenüber den Vorteil, daß eine unberechtigte Veränderung des Speicherinhalts des wiederbeschreibbaren Speichers zuverlässig erkannt werden kann. Es bietet daher einen guten Schutz gegen unberechtigte Manipulationen des Speicherinhalts.

Durch die in den abhängigen Ansprüchen aufgeführten Maßnahmen sind vorteilhafte Weiterbildungen und Verbesserungen des Verfahrens bzw. des Mikrorechners nach den unabhängigen Patentansprüchen möglich. Durch die Ausführung des Überprüfungsprogramms bei jedem Start des Mikrorechners wird gewährleistet, daß immer ein korrektes Programm im wiederbeschreibbaren Speicher gespeichert ist. Als Ergebnis des Überprüfungsprogramms kann bei einer gefundenen Abweichung der Rechner dann gesperrt werden. Dabei können auch unterschiedliche Schlüssel für unterschiedliche Bereiche des wiederbeschreibbaren Speichers vorgesehen werden, so daß einzelne Bereiche zur Veränderung durch den Anwender freigegeben sind und andere Bereiche gesperrt sind. Hiermit wird ermöglicht, ein verbessertes Programm oder optimierte Datenwerte im Feld, d. h. von Servicediensten nachprogrammieren zu lassen ohne aber hierdurch die Möglichkeit zu geben, daß Tuningfachleute, welche diese Programme erhalten, hieraus modifizierte Programme oder Daten erzeugen und abspeichern können mit anschließender Funktion der Elektronik.

Zeichnungen

Ausführungsbeispiele der Erfindung sind in den Zeichnungen dargestellt und in der nachfolgenden Beschreibung näher erläutert. Es zeigen

Fig. 1 einen Mikrorechner und

Fig. 2 einen Programmablauf des Überprüfungsprogramms.

Beschreibung

In der **Fig.** 1 wird ein Rechner **1** gezeigt, der einen Rechnerkern (CPU) und mehrere Speicher **1, 4, 5** aufweist. Bei dem Speicher **3** handelt es sich um einen nur-Lesespeicher (ROM), beim Speicher **4** um einen Schreib-/Lesespeicher (RAM) und beim Speicher **5** um einen wiederbeschreibbaren Speicher (EPROM, FLASH-EPROM). In den Speichern sind Programmbefehle oder Daten gespeichert die durch den Rechnerkern **2** verarbeitet werden. Dabei sind je nach Art des Speichers unterschiedliche Daten oder Programme abgelegt. Der nur-Lesespeicher **3** enthält ein festgespeichertes Programm welches nur durch Herstellung eines neuen Speicherbausteins geändert werden kann. In diesem Speicher wird daher in der Regel ein Minimalprogramm abgelegt, welches die CPU **2** in die Lage versetzt Befehle zu verarbeiten, die in anderen Speichermedien insbesondere dem wiederbeschreibbaren Speicher **5** gespeichert sind. Der Schreib-/Lesespeicher **4** ist nur während des laufenden Betriebs des Mikrorechners **1** in der Lage Daten zu speichern und dient daher nur zur Ablage von Daten oder von Programmbefehlen während des laufenden Betriebs des Rechners. Auf die Speicherinhalte des Schreib-/Lesespeichers **4** kann besonders schnell zugegriffen werden, so daß teilweise auch Programme von anderen Speichermedien, beispielsweise aus dem nur Lesespeicher **3** oder dem wiederbeschreibbaren Speicher **5** in den Schreib-/Lesespeicher **4** übertragen werden, um von dort aus ausgeführt zu werden. Der wiederbeschreibbare Speicher **5**, der hier als EPROM oder FLASH-EPROM ausgeführt ist, enthält Programmabschnitte oder Daten, die im gewissen Rahmen veränderbar sein sollen. Dadurch wird es möglich den Mikrorechner **1** an unterschiedliche Aufgaben anzupassen. Dies ist besonders vorteilhaft, wenn der Mikrorechner **1** als Steuergerät für ein Kraftfahrzeug angewendet wird. Im nur-Lesespeicher **3** werden dann neben dem Minimalprogramm Steuerprogramme für den Motor abgelegt. Im wiederbeschreibbaren Speicher **5** werden dann Daten, beispielsweise Motorparameter abgelegt, auf die das Steuerprogramm zugreift. Weiterhin können zusätzlich Programmodule im wiederbeschreibbaren Speicher **5** abgelegt werden, die z. B. nicht bei jedem Steuergerät verwirklicht werden sollen. Es ist so möglich, ein Steuergerät für unterschiedliche Anwendungen zu verwenden. Die Steuerfunktionen, die für alle Anwendungen gleich sind, werden im nur-Lesespeicher **3** abgelegt, während die Programme oder Daten die sich bei den einzelnen Anwendungen unterscheiden, im wiederbeschreibbaren Speicher **5** abgelegt werden. Problematisch ist dabei jedoch, daß diese erhöhte Flexibilität mit dem Risiko erkauft wird, daß Unbefugte den Speicherinhalt des wiederbeschreibbaren Speichers **5** verändern. In der Anwendung bei Kraftfahrzeugen könnte so beispielsweise die Leistung des Motors durch einen Austausch von Daten im wiederbeschreibbaren Speicher **5** erhöht werden. Um eine derartige unerwünschte Manipulation am Speicherinhalt des wiederbeschreibbaren Speichers **5** zu verhindern, wird im nur-Lesespeicher **3** ein Überprüfungsprogramm vorgesehen, welches in der Lage ist den Inhalt des Speichers **5** auf derartige unzulässigen Änderungen zu untersuchen.

In der **Fig.** 2 werden Programmschritte dieses Überprüfungsprogramms dargestellt. Vor dem ersten Programmblock **10** des Überprüfungsprogramms erfolgen die notwendigen Maßnahmen, um die CPU **2** zur Bearbeitung von Programmen vorzubereiten. Dabei werden interne Register der CPU **2** auf Ausgangswerte gesetzt, und die CPU wird so in die Lage versetzt, Ein- und Ausgabeoperationen, die zur Bearbeitung von Befehle notwendig sind, vorzunehmen. Nach der Ausführung eines solchen Minimalprogramms bzw. ei-

ner derartigen Bootroutine werden dann in einem ersten Programmblock des Überprüfungsprogramms aus den im wiederbeschreibbaren Speicher **5** enthaltenen Daten ein Codewort ermittelt. Ein einfaches Beispiel für ein derartiges Codewort besteht in einer Checksumme. Es sollten jedoch aufwendigere mathematische Verschlüsselungsverfahren angewendet werden, die ohne genaue Kenntnis des Verschlüsselungsalgorithmus einem Unbefugten nicht erlauben, aus dem Inhalt des wiederbeschreibbaren Speichers **5** das Codewort zu ermitteln. In einem weiteren Programmblock **11** erfolgt dann ein Vergleich des so ermittelten Codeworts mit einem Vergleichscodewort, das im wiederbeschreibbaren Speicher **5** gespeichert ist. Wenn das Codewort und das Vergleichswort miteinander übereinstimmen wird das weitere Programm, hier durch den Programmblock **12** dargestellt, fortgesetzt. Wenn das Codewort und das Vergleichswort nicht übereinstimmen, wird das Steuergerät **1** für den weiteren Betrieb gesperrt.

Ein berechtigter Benutzer, der den Inhalt des wiederbeschreibbaren Speichers **5** ändern will wird somit mit dem nur ihm bekannten Verschlüsselungsalgorithmus aus dem im Speicher **5** abzulegenden Programm ein Vergleichscodewort ermitteln und diese dann mit dem Speicher **5** ablegen. Bei der Durchführung des Überprüfungsprogramms wird dann der Mikrorechner **1** ordnungsgemäß arbeiten. Eine unberechtigte Änderung des Speicherinhalts des wiederbeschreibbaren Speichers **5** scheitert daran, daß der Verschlüsselungsalgorithmus nicht bekannt ist, so daß es dann nicht möglich ist, im wiederbeschreibbaren Speicher S ein korrektes Vergleichscodewort abzulegen. Durch das Überprüfungsprogramm wird dann der Mikrorechner **1** für die Bearbeitung weiterer Aufgaben gesperrt. Unerwünschte Manipulationen am Speicherinhalt des wiederbeschreibbaren Speichers **5** sind somit zuverlässig unterdrückt.

Das Überprüfungsprogramm kann auch so ausgelegt werden, daß nur einzelne Bereiche des Speichers **5** überprüft werden. Weiterhin ist es möglich, das Überprüfungsprogramm so auszulegen, daß für unterschiedliche Bereiche des wiederbeschreibbaren Speichers **5** unterschiedliche Verschlüsselungsalgorithmen angewandt werden und für jeden dieser Bereiche ein eigenes Codewort abgelegt wird. Es können so einzelne Bereiche des wiederbeschreibbaren Speichers **5** wahlweise für eine Neuprogrammierung gesperrt werden oder wahlweise freigegeben werden.

Weiterhin ist es auch möglich statt einer kompletten Sperrung des Mikrorechners **1** bei einer Abweichung von Codewort und Vergleichscodewort eine nur teilweise Sperrung vorzusehen. Wenn beispielsweise der Mikrorechner **1** als Motorsteuergerät verwendet wird, kann vorgesehen werden, daß bei einer unberechtigten Manipulation des Kennfeldes für den Zündwinkel statt einer Sperrung der Funktion ein Zündwinkel herangezogen wird, der noch einen leistungsverminderten Betrieb des Motors erlaubt und gleichzeitig eine Aufforderung auslöst, das Fahrzeug bei einer Werkstatt reparieren zu lassen. Es kann so sichergestellt werden, daß auch bei einer zufälligen Veränderung des Inhalts des Speichers **5** noch eine gewisse Minimalfunktion des Mikrorechners ausgeübt wird.

Weiterhin ist es möglich das Überprüfungsprogramm zunächst in einem inaktiven Zustand zu lassen und so zunächst noch Veränderungen des Speicherinhalts des wiederbeschreibbaren Speichers zuzulassen. Dies ist insbesondere für eine Entwicklungsphase, bei der noch häufig Modifikationen des im wiederbeschreibbaren Speichers gespeicherten Programm erforderlich sind von Vorteil. Nach dem Ende der Entwicklung wird dann durch die Aktivierung des Überprüfungsprogramms sichergestellt, daß weitere Manipulationen nur mit Kenntnis des Schlüssels möglich sind.

Patentansprüche

1. Verfahren zum Schutz eines Mikrorechners (**1**) gegen Manipulation seines Programms, wobei der Mikrorechner einen nur-Lesespeicher (**3**) und einen wiederbeschreibbaren Speicher (**5**) aufweist, wobei mindestens ein Teil des Programms in dem wiederbeschreibbaren Speicher (**5**) gespeichert wird, **dadurch gekennzeichnet**, daß ein im nur Lesespeicher (**3**) enthaltenes Überprüfungsprogramm (**10, 11**) ausgeführt wird, bei dem mit einem Schlüssel aus zu mindestens einem Teil des im wiederbeschreibbaren Speichers (**5**) enthaltenen Speicherinhalts ein Codewort ermittelt und mit einem im wiederbeschreibbaren Speicher (**5**) abgelegten Vergleichscodewort verglichen wird.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das Überprüfungsprogramm (**10, 11**) bei jedem Start des Mikrorechners (**1**) ausgeführt wird.
3. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß bei einer Übereinstimmung des Codewort und des Vergleichscodewort der Mikrorechner (**1**) zur Ausführung weiterer Programme freigegeben und bei einer Nichtübereinstimmung von Codewort und Vergleichscodewort der Mikrorechner (**1**) zumindest teilweise gesperrt wird.
4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß das Überprüfungsprogramm mindestens zwei Schlüssel aufweist und daß jeder Schlüssel zur Bildung eines Codeworts eines ihm zugeordneten Bereich des wiederbeschreibbaren Speichers (**5**) zugeordnet ist.
5. Geschützter Mikrorechner (**1**) mit einem nur Lesespeicher (**3**) und einem wiederbeschreibbaren Speicher (**5**) wobei im wiederbeschreibbaren Speicher (**5**) ein Programm gespeichert ist, dadurch gekennzeichnet, daß im nur Lesespeicher (**3**) ein Überprüfungsprogramm (**10, 11**) gespeichert ist, daß das Überprüfungsprogramm (**10, 11**) in Abhängigkeit vom Inhalt des wiederbeschreibbaren Speichers (**5**) ein Codewort bildet und dieses Codewort mit einem im wiederbeschreibbaren Speicher (**5**) abgelegten Vergleichscodewort vergleicht.
6. Mikrorechner nach Anspruch 5, dadurch gekennzeichnet, daß der Mikrorechner bei jedem Start eine Bootroutine ausführt und daß das Überprüfungsprogramm Teil dieser Bootroutine ist.
7. Mikrorechner nach Anspruch 5 oder 6, dadurch gekennzeichnet, daß bei einer Nichtübereinstimmung von Codewort und Vergleichscodewort die Abarbeitung weiterer Befehle durch einen Rechnerkern (**2**) gesperrt wird.
8. Mikrorechner nach Anspruch 5 bis 7, dadurch gekennzeichnet, daß mehrere Schlüssel vorgesehen sind, die jeweils einem Bereich des wiederbeschreibbaren Speichers (**5**) zugeordnet sind, und daß mehrere Vergleichscodewörter im wiederbeschreibbaren Speicher (**5**) vorgesehen sind, die jeweils einem der Speicherbereiche zugeordnet sind.
9. Mikrorechner nach Anspruch 5 bis 8, dadurch gekennzeichnet, daß der wiederbeschreibbare Schreiber (**5**) als Flash-Speicher ausgebildet ist.
10. Mikrorechner nach Anspruch 5 bis 8, dadurch gekennzeichnet, daß der nur Lesespeicher (**3**) ein spezieller Bereich im Flash-Speicher ist.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 197 23 332 A1
Int. Cl.[6]: G 06 F 12/14
Offenlegungstag: 3. September 1998

Fig. 1

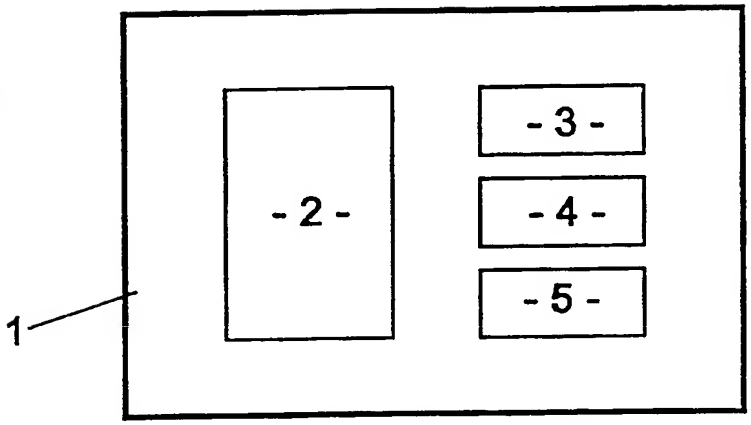
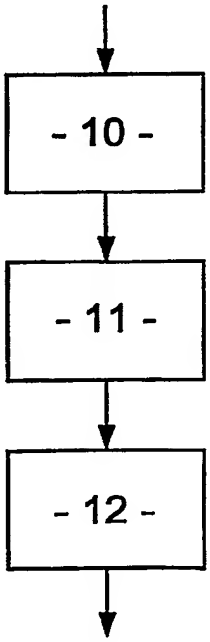


Fig. 2



802 036/354